PREMIERS PAS VERS VOTRE CONFORMITÉ AU RGPD

Le règlement général sur la protection des données (RGPD) est entré en vigueur le 25 mai 2018. Le règlement apporte de nouveaux droits aux personnes physiques et de nouvelles obligations aux entreprises.

Les données personnelles comprennent toutes les informations qui se rapportent à une personne physique identifiée ou identifiable (telles que le nom, l'adresse, le numéro de téléphone, l'adresse e-mail, le numéro personnel, les plaques d'immatriculation, etc.).

CARTOGRAPHIER LES DONNÉES DE VOS CLIENTS ET DE VOS EMPLOYÉS

Dans un premier temps, il est important de définir les différents traitements de données (p.ex. gestion des ressources humaines, tenue d'un fichier clients, etc.). Pour chaque traitement, il faut documenter quelles données personnelles vous détenez, quelles sont les finalités du traitement, où sont stockées ces données, si une procédure de suppression est prévue, et quelles personnes y ont accès.

Une fois ce travail de cartographie effectué, vous devez vous poser les questions suivantes :

? QUESTION	! EXPLICATION
Est-ce que je ne collecte pas plus de données que nécessaire ? Est-ce que je ne les garde pas plus longtemps que nécessaire ?	Seules les données nécessaires (et pas les données seulement utiles) doivent être collectées **(principe de minimisation)**. La question à se poser est de savoir pourquoi est-ce que je collecte telle ou telle donnée? Ai-je besoin de ces données pour offrir mon produit ou service ? Un autre principe à respecter est le **principe de la durée de conservation limitée.** Pour respecter ce principe, la question à se poser est de savoir s'il existe des obligations légales de conservation (par exemple, 10 ans pour les factures émises) ? Assurez-vous ensuite que ces données sont exactes et à jour. Si ce n'est pas le cas, les données erronées doivent être effacées ou corrigées **(principe d'exactitude)**. Selon le RGPD, des mesures actives doivent être prises pour supprimer les informations dès qu'elles ont perdu leur pertinence. Des arguments tels que „cela pourrait être utile un jour" ou „on ne sait jamais" ne sont donc pas valables. Les informations collectées ne peuvent être utilisées que dans le but pour lequel elles ont été collectées et ne peuvent pas être conservées plus longtemps que nécessaire.
Est-ce que le traitement des données personnelles est légal ?	Le traitement des données personnelles n'est légal que s'il entre dans une des hypothèses suivantes **(principe de licéité)*** : • une obligation légale (exemple: données récoltées pour une déclaration sociale ou fiscale) • l'exécution d'un contrat ou de mesures précontractuelles (exemple: gestion d'un contrat de travail, ou établissement d'un devis) • l'intérêt légitime du responsable de traitement (cet intérêt doit cependant être confronté aux droits et libertés de la personne concernée) ** L'intérêt public et l'intérêt vital de la personne sont deux autres conditions qui permettent le traitement des données personnelles. Cependant, celles-ci sont moins pertinentes dans l'Artisanat.* Si votre traitement de données ne se fonde sur aucune des finalités énoncées ci-dessus, vous devez obtenir un consentement de vos clients. Si la personne concernée accepte le traitement, elle doit le faire activement (par exemple en cochant une case). Vous devez ensuite documenter ce consentement pour pouvoir le mettre à disposition des autorités nationales de la protection des données ou de la personne concernée sur demande.

QUESTION	EXPLICATION
La personne concernée est-elle au courant du traitement ? Est-ce que je peux respecter son droit d'accès et son droit à l'oubli ?	Expliquez, dans un langage clair et simple, quelles données personnelles vous traitez, pour quelle raison et pour quelle durée, et si elles sont transmises à un soustraitant **(principe de transparence).** Veillez à ce que, sur demande d'une personne concernée, vous pouvez mettre à sa disposition une copie de l'intégralité des données que vous possédez la concernant et que vous êtes en mesure de supprimer ces données le cas échéant. Dès qu'une personne demande des informations sur les données stockées la concernant, vous devez les lui fournir le plus rapidement possible. Soyez donc bien préparé, lorsque vos clients vous demandent quelles informations vous détenez sur eux. En outre, les personnes concernées ont le « droit à l'oubli ». Cependant, tant que vous avez des obligations légales à respecter ou que la conservation des données est nécessaire pour exécuter votre métier, vous n'avez pas besoin de les supprimer. Si la suppression n'est pas possible pour des raisons techniques, les données doivent être anonymisées afin que la personne concernée ne puisse plus être identifiée, même pas par vous-même.
Les données personnelles sont-elles stockées en toute sécurité ?	Le stockage sécurisé des informations personnelles est de votre responsabilité. Ceci inclut, entre autres, le transfert de vos données à des tiers (par exemple, fournisseurs, comptabilité externe, fournisseurs de cloud). Par conséquent, assurez-vous que la protection des données et la sécurité du stockage sont aussi importantes pour vos partenaires contractuels que pour vous. Si vous échangez de nombreuses données personnelles avec vos partenaires, vérifiez les clauses de protection des données et les responsabilités correspondantes dans vos contrats. Dès que vous prenez connaissance d'une atteinte à la protection des données, qui menace les droits et libertés des personnes impliquées, vous devez la signaler à la Commission nationale de protection des données (CNPD) dans un délai de 72 heures.
Est-ce que je dois nommer un délégué de la protection des données (DPO) ?	Le DPO veille à la mise en œuvre et au respect du RGPD au sein de votre entreprise et agit en tant que personne de contact pour tous renseignements et toutes plaintes des personnes concernées. La nomination d'un délégué à la protection des données est obligatoire pour : • les organismes publics • les entreprises dont l'activité de base exige un suivi régulier et systématique à grande échelle de personnes, ou dont l'activité de base consiste à traiter à grande échelle des données sensibles. Dans les autres cas la désignation d'un DPO est facultative.
Est-ce que je suis tenu d'avoir un registre des activités de traitement ?	Le registre des activités de traitement n'est pas obligatoire pour les entreprises avec moins de 250 salariés, sauf si le traitement des données personnelles est risqué, pas occasionnel ou concerne des informations sensibles ou juridiques. Si un tel registre ne vous est pas imposé, il faut souligner que la tenue d'un fichier qui reprend l'ensemble de vos traitements est nécessaire pour toute entreprise afin d'avoir un aperçu clair des différents traitements et de respecter vos obligations de documentation. En effet, vous devrez être capable de démontrer, sur demande, que votre traitement de données est légal et conforme au RGPD.

La Commission nationale de protection des données (CNPD) a publié une brochure destinée à sensibiliser le public sur le nouveau règlement. Le but de cette brochure est de présenter les droits des citoyens en matière de protection des données et d'expliquer comment les faire valoir. La brochure est disponible en versions allemande et française et peut être téléchargée sur le site internet du CNPD (www.cnpd.lu).

REMARQUE: la rédaction de cette fiche d'information a été faite avec le plus grand soins.
Toutefois, toute responsabilité concernant les erreurs éventuelles qui y seraient contenues est déclinée.

CHAMBRE DES METIERS
Luxembourg

YDÉ
BIEN ENTOURÉ POUR RÉUSSIR VOS PROJETS

Vous avez des questions ?
Vous souhaitez recevoir plus d'informations sur la digitalisation ?
Contactez le Service eHandwierk de la Chambre des Métiers :
Tél. : 42 67 67 - 305 / 306 | **E-Mail :** ehandwierk@cdm.lu